学校编码：10384　　分类号_____密级_____

学号：X2012231181　　UDC _____

工　程　硕　士　学　位　论　文

涉密信息网络管理监控系统的设计与实现

Design and Implementation of Supervisory and Management System for Confidential Information Network

周思思

指 导 教 师：　龙 飞 副教授

专 业 名 称：　软 件 工 程

论文提交日期：　2014 年 10 月

论文答辩日期：　2014 年 10 月

学位授予日期：　　年　月

指　导　教　师：_____

答辩委员会主席：_____

2014 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为(　　)课题(组)的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

随着信息技术的发展，计算机和网络技术的应用已经渗透到日常生活中的各个角落。这些信息技术给我们生活带来便捷的同时，由于网络和计算机的特性，也导致信息、数据容易被窃取和从内部泄漏。

本课题以涉密信息网络管理为对象，设计并实现涉密信息网络管理监控系统。课题围绕着涉密信息网络管理监控系统的设计与实现，采用 C/S 模式、Visual Studio 集成开发环境进行系统的研发工作。笔者首先结合信息安全和软硬件开发理论，针对目标系统所需要解决的问题进行了详细的需求分析；接着采用快速开发和便于维护的结构化开发方法，进行了详细的系统设计，提出了详细的解决方案和系统应用架构，并给出详细的系统实现。

目标系统涵盖了下级中心设置、预警中心设置、告警设置、生成注册器、管理注册客户端、内网客户端扫描、客户端注册、USB 设备加密、违规告警等核心功能模块。本系统可以有效监控涉密计算机和涉密网络，防止涉密信息外泄，保证涉密信息与互联网的物理隔离，避免涉密信息通过非授权移动存储设备流出，杜绝未授权电脑对涉密网络，特别是重点服务器的访问。

关键词：信息安全；涉密信息网络；C/S

Abstract

With the development of information technology, the application of computers and network technology has penetrated into every corner of daily life. The information technology brings convenience to our life but they make information and data easy to be stolen and be leaked from the internal due to the characteristics of network and computer at the same time.

This thesis uses confidential information network management as an object, designs and implements confidential information network management monitoring system. Thesis is surrounding the designs and implementation of confidential information network management monitoring system and using C/S mode and Visual Studio integrated development environment for the development of the system. The author first combines the theory of information and the hardware and software development theory, and carried out a detailed demand analysis for the problems which the target system needs to solve, and then use rapid development and easy maintained structured development methods to make detailed system designs, and put forward the detailed solutions and system application architecture, and give the detailed system implementation.

The target system has lower center settings, warning center settings, alarm settings, production registrar, registered client management, intranet client scanning, client register, USB device encryption, violation alarm and other core function modules. This system can monitor confidential computer and internet effectively, prevent confidential information from leakage, guarantee the physical isolation between confidential information and Internet, avoid leaking the confidential information by the unauthorized removable storage device, completely eradicate unauthorized computer visiting the confidential internet especially the key servers.

Keywords: Information Security; Confidential Information Network; C/S

目录

Contents

第一章 绪论

1.1 课题背景

信息化技术的飞速发展，使得计算机和网络技术的应用已经渗透到了日常生活中的各个角落[1,2]。由于网络和计算机信息系统固有特性，先进的网络及其应用技术一方面给企业带来工作和管理高效率，提高了数据和信息的共享性，另一方面却也使得企业信息、数据容易被非法窃取、复制和使用[3]。为了防止信息外泄，企业、政府部门不惜重金购进防火墙、杀毒、入侵检测等网络安全产品和软件，但是根据权威资料记载，大部分的机密、敏感数据，85%以上都是由于内部员工合法或者非法手段泄漏，而且呈上升趋势[4]。因此，政府部门和企业当前急需解决“如何防止企业内部员工、外来者有意或者无意的操作将涉及国家机密以及企业内部敏感数据外泄”这一安全问题。

2000 年 1 月 1 日起国家保密局规定，“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相连接，必须实行物理隔离”。为了规范涉密计算机的管理，国家保密局结合当前涉密信息系统建设的现状，要求涉密计算机必须配备具有“违规外联监控”、“涉密移动存储介质使用管控”和“非涉密信息单向导入”等功能的专用保密防护系统，也即“三合一”系统。

基于以上背景，本课题从维护涉密计算机和涉密网络的信息安全为出发点，以适应新的涉密信息监控技术为目标，研发了涉密信息网络管理监控系统，以便应对日益复杂的信息外泄方式，更加有效的监控涉密计算机和涉密网络，防止涉密信息外泄，保证涉密信息与互联网的物理隔离，避免涉密信息通过非授权移动存储设备流出，杜绝未授权电脑对涉密网络，特别是重点服务器的访问。

1.2 研究现状

目前信息泄漏的途径多种多样，例如，在企业内部，可能通过 USB 接口拷贝到 U 盘等移动存储设备中、可能通过网络把信息传输出去、也可能通过邮件发送到外部或者通过打印把电子文档转成纸质带走等等多种途径[5,6]。从总体上

来说，信息泄漏的方式可分为三种：计算机网络化造成的信息泄漏、计算机外设结构造成的信息泄漏、移动存储设备造成的信息泄漏[7]。

针对以上三种信息泄漏方式，目前涉密信息防泄漏的主要保护手段可分为三重。第一重：详尽细致的操作审计；第二重：全面严格的操作授权；第三重：安全可靠的透明加密[8]。这三重保护实则属于防信息被动泄漏技术。防信息被动泄漏技术的主要手段就是加强对用户的安全认证和对涉密计算机的涉密数据存储的加密。从广义上说，信息防泄漏技术还存在一种防信息主动泄漏技术，因为防信息主动泄漏技术的主体是被授权访问涉密信息的内网用户，而且具有相关操作的权限，故相比防止信息被动泄漏技术，防信息主动泄漏技术更加复杂。

目前关于涉密信息监控的技术和产品主要包括：针对计算机网络化的信息泄漏的防护与监控、针对外设接口造成的信息泄漏的防护与监控和针对移动存储设备造成的信息泄漏的防护与监控。但却没有一种“三合一”产品对涉密信息进行监控和防护。并且随着信息载体的多样化、违规方式的多样化，涉密信息网络管理已经不仅仅是违规外联的监控，违规内联、非授权存储设备使用的监控要求亦日益迫切。反监控手段的进步也要求采取更为先进的技术来达到监控的目的。

1、随着杀毒软件和防火墙的不断更新和升级。进程守护技术开始被部分杀毒软件当成病毒。在报警数据通过防火墙时，会弹出是否允许通过防火墙的对话框，在用户选择阻止的情况下，报警数据包将被阻断，达不到预期的目的。

2、涉密单位内部网络的重点服务器存有重要的涉及国计民生的重要信息，必须保证访问它的每一台电脑都是经过授权的。

3、移动存储设备（U 盘，移动硬盘）在日常生活中已经被广泛的使用，涉密电脑上必须保证使用的外接设备是经过授权的，杜绝非授权移动存储设备在涉密电脑上的使用，在服务器能够对每台涉密电脑的 USB 接口做到读写控制，对其的使用能够做到全面的记录。

4、在违规外联的同时，也会有非授权电脑违规接入内部涉密网络。这种行为同样危险。在违规内联时，能够被发现和阻止，并向服务器报警。

5、当涉密计算机非法访问互联网时，要求更准确的了解用户接入时的行为和定位用户违规时的地理方位。

6、涉密电脑和内部网络违规方式的多样化复杂化，反监控技术的高端化，要求程序具有优秀的升级补丁的能力，做到一次安装，终生免疫。

本课题研发的涉密信息网络监控系统将通过在涉密计算机注册客户端，当被监控计算机违规接入互联网时，客户端能够及时发现和采取断网、关机等策略，并向处于互联网的预警中心发送该机的违规信息。只要用户注册了客户端监控程序，无论在什么地方，无论什么时间接入外网都可以达到监控的目的。通过预警中心显示的报警信息，可以非常容易的定位处违规计算机的区域、单位、用户等。

1.3 课题主要研究内容与目标

本课题的主要研究内容是：

1、对接入内部网络的计算机进行强制注册，当涉密计算机违规接入互联网或外部计算机未经授权访问内部网络时能够实时监控、记录、告警并阻止。

2、对涉密计算机接入的移动存储设备进行监控，在服务器端可以对客户端外设接口进行控制。有新的补丁时自动升级。

3、在涉密主机注册的程序能够隐藏，自身防删除，在报警时不被防火墙阻挡。对涉密计算机的 CPU，硬盘，主板，网卡等进行户口簿式的管理。

涉密信息网络管理监控系统集中实现阻断涉密计算机违规外联、防止移动存储介质交叉使用、非涉密信息单向导入涉密计算机这三方面的功能。系统能够有效的解决涉密计算机及移动存储介质保密管理薄弱、泄密事件高发的问题，能够切实解决涉密计算机违规连接互联网和移动存储介质在涉密计算机与非涉密计算机之间交叉使用引起的安全保密问题。

在涉密信息网络管理监控系统项目中，主要以完成客户端程序强制注册，隐蔽运行，被停止后自动重启，防删除，报警穿透防火墙，对非授权计算机访问涉密网络的阻断和报警等功能。以能满足现今技术条件下对涉密计算机和网络的全方位，全天候，多功能监控为最终目的。

本课题的研究目标是：

1、 以全面监控涉密电脑外联互联网情况，有效防止信息通过互联网外泄为目标。

2、以全面监控涉密网络非授权访问情况，有效防止非授权电脑接入内部网络为目标。

3、以全面监控涉密电脑的移动存储设备使用情况，有效防止移动存储设备的滥用。

4、 严把时效关，将及时报警和处置置于突出的重要位置优先考虑，优先安排，确保工程质量。同时注意技术文档资料的积累保管，确保工程经得起时间的检验。

1.4 章节安排

本文主要由六章组成，各章内容介绍如下：

第一章绪论。对课题背景、研究现状以及课题的主要研究内容进行概要性描述。

第二章系统相关理论基础及开发技术介绍。主要介绍系统相关理论和开发技术。

第三章系统需求分析。主要介绍系统需求分析方面的内容。具体包括系统可行性分析、系统业务需求、功能性需求和非功能性需求等。

第四章系统设计。主要介绍系统设计方面的内容。从系统总体设计、功能模块设计、出错设计、安全保密设计等内容，给出系统设计方案。

第五章系统的实现。介绍系统功能特点；给出关键技术解决方案和部分功能实现。

第六章总结与展望。指出该课题的成果、不足和下一步的工作。

第二章 系统相关理论基础及开发技术介绍

本章的主要内容是介绍系统相关理论知识和开发技术。系统相关理论知识主要包括信息安全、涉密信息系统和涉密信息网络管理监控的功能等。开发技术主要包括 C/S 模式、Visual Studio 集成开发环境和 ADO.NET 数据库访问技术。下面为本章详细内容。

2.1 相关理论介绍

2.1.1 信息安全的概念

信息安全是指信息系统受到保护，不受到恶意或者非恶意的因素遭到泄漏、修改或者破坏，保证信息服务不可断、系统连续可靠地运行，从而最终实现业务连续性[9]。这里的信息系统包括软硬件、数据、物理环境、基础设施和人等。根据国际标准化组织关于信息安全的定义，则指出信息安全的含义主要指信息可用性、完整性、保密性以及可靠性[11]。信息安全主要包括保证信息的完整性、真实性、保密性、所寄生系统的安全性以及未授权拷贝等五个方面的内容。信息安全的目的是使内部信息不受内部、外部以及自然等因素的干扰与威胁。为了保障信息安全，要求有信息源认证、访问控制、防止非法软件驻留、防止未授权操作等行为。

信息作为资源，包括普遍性、共享性、多效性、可处理性和增值性等五种属性[10]，这些属性使得信息对于人类具有及其重要的意义。信息安全是信息的本质属性所体现的安全意义，现代信息安全主要包括运行系统的安全、系统信息的安全和信息内容的安全等三层含义[12]。信息安全的本质就是保护计算机信息系统或者计算机网络中的信息免受各种类型的威胁、干扰和破坏。

2.1.2 涉密信息系统的概念

计算机的信息系统包括信息系统和信息管理。它是指由计算机及其相关和配套设备、设施构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。